20-MJ-7069-JCB

AFFIDAVIT OF JASON J. DEFREITAS IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Jason J. DeFreitas, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security ("DHS") United States Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") assigned to the Boston Field Office and have been employed by HSI since 2006. I am currently assigned to the Cyber Group. Prior to my assignment to the Boston Field Office, I was assigned to the HSI Los Angeles Field Office, where I served as a member of the Intellectual Property Rights Group. In connection with my official duties, I have investigated and assisted other agents in investigating cases involving a wide variety of criminal violations including, but not limited to, fraud, intellectual property rights, cultural property theft, and child pornography. Prior to my employment with ICE HSI, I served as a United States Customs and Border Protection ("CBP") officer at the Los Angeles International Airport for approximately four years. My duties included the interception and examination of individuals and merchandise for violations of United States.

2. I have been involved in an investigation of Garry Bienvenue, born 1962, involving Receipt of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A), and Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B) (the "SUBJECT OFFENSES"). On or about March 11, 2020, this Court authorized a search warrant for Bienvenue's residence located at 23 4th St, Apt. 2, Attleboro, Massachusetts, 20-MJ-7050-JCB (the "Attleboro Residence Warrant") to search for evidence, instrumentalities, fruits of a crime and contraband of the SUBJECT OFFENSES.

3. I submit this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure, as well as Title 18, United States Code, Sections 2703(a),

2703(b)(1)(A) and 2703(c)(1)(A) to search and seize the following Dropbox account, as described more fully in Attachment A, including the contents of communications, associated with email address **gbowler47@gmail.com** (the "SUBJECT DROPBOX ACCOUNT"). Dropbox has informed me that it accepts service of process at 1800 Owens Street, Suite 200, San Francisco, CA 94158, and via the email address legalcompliance@dropbox.com. Dropbox is headquartered at the China Basin Landing Building, 185 Berry Street, Suite 400, San Francisco, California, 94107-1739. The evidence described in Attachment B includes evidence maintained in electronic format within the SUBJECT DROPBOX ACCOUNT. The methods by which the electronic information will be searched are more fully set forth in the "TECHICAL BACKGROUND REGARDING DROPBOX" section of this affidavit.

4. As described herein, there is probable cause to believe that the user of the SUBJECT DROPBOX ACCOUNT has committed the SUBJECT OFFENSES, and the content of SUBJECT DROPBOX ACCOUNT will contain evidence of a crime, contraband, fruits of crime, or other items illegally possessed.

5. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing the requested search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the requested search warrant.

STATEMENT OF PROBABLE CAUSE

6. On or about March 12, 2020, I participated in the execution of the Attleboro Residence Warrant. During the course of the search, several electronic devices were seized, including a LG V30, serial number 804KPKN211133 (the "LG Phone") which Bienvenue

acknowledged belonged to him and provided the swipe pattern to unlock. Agents conducted a preliminary, on-scene forensic preview. During the course of that preview, agents located four videos depicting child pornography located on the LG Phone. Certain of those files are described as follows:

a. Snapchat-2050713481.mp4 – This video is approximately 1 minute and 17 seconds in length, and depicts a nude prepubescent female child, approximately 3 to 5 years old, laying on her back on a white sheet. At first the camera only shows the female child from the waist up. At approximately 49 seconds into the video, the camera pans down and shows her vagina. An erect penis is seen being repeatedly inserted into the female child's vagina. At approximately 1 minute and 2 seconds into the video, the erect penis appears to ejaculate onto the female child's stomach. This file was located at file path /sdcard/Snapchat. The modified date for the file is 10/2/2019 2:11:58 AM (UTC+0).

b. Snapchat-1471833041.mp4 – This video is approximately 8 seconds in length and depicts a prepubescent female child, approximately 4-6 years old, laying on her side with her pants and underwear pulled down to her thighs. The camera is focused in on her anus and vagina, and an adult hand is spreading her buttocks apart to further expose her anus. As the video plays, the camera focuses very close to her exposed anus and vagina, and then pans back out farther away. This file was located at file path /sdcard/Snapchat.

7. This court reviewed still images from the two videos described in paragraphs 6(a) and 6(b) prior to issuing the Criminal Complaint in this matter, 20-MJ-7060-JCB, and found probable cause to believe that the images depict minors engaged in sexually explicit conduct.

8. Agents also were able to determine that the Dropbox application and a user account for the SUBJECT DROPBOX ACCOUNT, gbowler47@gmail.com, was on the LG Phone. Bienvenue executed a written consent form permitting agents to search his Dropbox account along with two other messenger accounts.

9. After being advised of and executing a written waiver of his Miranda rights, Bienvenue agreed to speak with investigators. Among other things, Bienvenue admitted to storing child pornography on the SUBJECT DROPBOX ACCOUNT.

10. Pursuant to Bienvenue's written consent, agents accessed the SUBJECT DROPBOX ACCOUNT and observed hundreds of videos of pornography. I participated in preview of the videos on scene and believe that majority of the videos in the SUBJECT DROPBOX ACCOUNT contain child pornography. Specifically, I participated in the preview of approximately 10 videos found in the SUBJECT DROPBOX ACCOUNT and these videos contain what I believe constitutes child pornography. These videos depict children who appeared to be approximately six to twelve years old. One of these files is described as follows:

a. "Snapchat-310235069.mp4" is a video that is approximately 17 seconds in duration and depicts a nude, prepubescent female child between the ages of 6-9 years old. In this video the child's breasts and vagina are visible. During the video the child is lying down and places her legs behind her head. At one point of the video, the child positions herself so her exposed vagina is fully visible within the frame of the video.[1]

[1] I have not provided a still image from this video for the court's review because that is not necessary to establish probable cause under the circumstances of this case. I am aware that the "preferred practice" in the First Circuit is that a magistrate judge view images relied upon for the issuance of a search warrant in this context, to determine whether the images depict the lascivious exhibition of a child's genitals. *United States v. Brunette*, 256 F.3d 14, 19 (1st Cir. 2001). Here, however, the descriptions offered "convey to the magistrate more than [my] mere opinion that the images constitute child pornography." *United States v. Burdulis*, 753 F. 3d 255, 261 (1st Cir. 2014) (distinguishing *Brunette*). Additionally, because the defendant admitted to storing child pornography on the

11. Based on the foregoing information, I submit that there is probable cause to believe that the content of the SUBJECT DROPBOX ACCOUNT will contain evidence of a crime, contraband, fruits or crime, or other items illegally possessed. Specifically, I submit that based upon the recovery of child pornography from Bienvenue's LG Phone, Bienvenue's statements, and the files observed during the on-scene search of the SUBJECT DROPBOX ACCOUNT, there is probable cause that the SUBJECT DROPBOX ACCOUNT will contain video and image files depicting child pornography.

TECHNICAL BACKGROUND REGARDING DROPBOX

12. Dropbox, a Remote Computer Services Provider,[2] is a file hosting service operated by Dropbox, Inc., headquartered in San Francisco, California, that offers cloud storage, file synchronization, personal cloud, and client software. Dropbox allows users to create a special folder on each of their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer is used to view it. Files placed in this folder also are accessible through a website and mobile phone applications.

13. Dropbox users sign up for an account with a valid e-mail address. To sign into the user's Dropbox account, the user enters an email address and password. Dropbox will typically give users a certain amount of free storage, and if the user wants more storage, the user can pay for it. Users can access Dropbox from anywhere in the world using the internet and avoid having the files appear on the user's computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if the user opted to store them at an offsite location

SUBJECT DROPBOX ACCOUNT, and the magistrate judge has already viewed still images of videos stored on the LG Phone and found probable cause to believe that the images depict minors engaged in sexually explicit conduct, the magistrate judge's viewing of additional images is not necessary to find probable cause to issue the requested warrant.

[2] As defined by 18 U.S.C § 2711, "the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system."

such as Dropbox. For example, a user can take a photograph from a smartphone, upload that photo to Dropbox, and erase it from their phone. The photograph now resides in the user's "cloud." The user can then access his/her Dropbox account from a desktop computer and download the photograph to that machine.

14. Dropbox provides a variety of online services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information ("PII"), which can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email address(es), and means and source of payment, including any credit or bank account number (for paying customers).

15. Another feature of Dropbox is sharing. A Dropbox user can share certain files he/she designates by sending a web link to another user. It then gives the second user access to those particular files.

16. I know that Dropbox maintains records on their users, such as basic subscriber information within the meaning of 18 U.S.C. § 2703(c)(2). Furthermore, I know Dropbox keeps and maintains the stored content of their users' accounts, such as photographs, movies, documents, and music, all within the meaning of the Stored Communication Act.

17. According to Dropbox's privacy policy, at https://www.dropbox.com/privacy (last visited March 24, 2020), Dropbox collects and stores:

> "[user's] name, email address, phone number, payment info, and physical address;"
>
> "[user's] files, documents, photos, comments, messages, and so on;"

> "things like the size of the file, the time it was uploaded, collaborators, and usage activity…like sharing, editing, viewing, and moving files or folders;"
>
> "Information from and about the devices…use[d] to access the Services…like IP addresses, the type of browser and device…use[d], the web page…visited before coming to our sites, and identifiers associated with [user's] device."

18. Based on my training and experience, I know that electronic communication services and remote computing services such as Dropbox retain business records and subscriber information such as account applications, subscribers' full names, all screen names associated with the subscribers and/or account, all account names associated with the subscribers, services available to the subscriber, methods of payment, telephone numbers, addresses, passwords, and detailed billing records.

19. Based on my training and experience, I also know that electronic communication services and remote computing services such as Dropbox maintain electronic records pertaining to the individuals and companies for whom they maintain subscriber accounts including account access information, email transaction information, and account application information, email communications, and image files.

20. Through my training and experience, I know that private citizens and businesses are using electronic service providers ("ESPs") who provide the service of storing data from anywhere there is a connection to the internet, commonly known as cloud-based storage. This allows the customer to connect to the server and view, alter, create, copy, and print the data from the remote server as if it was at the same location as the user. The user typically owns and controls the data stored at the remote server while the ESP owns the server on which the data is stored.

21. As in the instant case, law enforcement typically does not find out about the existence of the remote server. Law enforcement cannot access or view this cloud-based data unless they know it exists and have access to a remote computer capable of connecting to and authenticating the user's cloud-based account. Witnesses and informants who have access to the data also typically do not know where the data is stored.

22. The server may be located in another city or state from the site of the initial service, making it difficult for law enforcement to preserve the evidence in a traditional manner. It takes hours and sometimes days to determine the location of the remote server and gather the details containing the specificity necessary for the issuance of a second search warrant. Depending on the size of the evidence, a suspect can delete it from a system within seconds using a smart phone or another internet capable device at any location. A forensic examiner often can recover evidence suggesting whether a computer (including a computer, cell phone, tablet, or other internet capable device) was used to access data which had been stored on a remote server in a cloud storage account. Such information is often maintained indefinitely until overwritten by other data.

23. Based upon the initial review of the content of the SUBJECT DROPBOX ACCOUNT, I sent Dropbox a letter on March 20, 2020, requesting under 18 U.S.C § 2703(f) that the company preserve records associated with the SUBJECT DROPBOX ACCOUNT for a period of 90 days.

24. In general, content that is sent to a Dropbox account is stored in the subscriber's "user account" on Dropbox servers until the subscriber deletes the content. If the subscriber does not delete the content, the content can remain on Dropbox's servers indefinitely. Even if the subscriber deletes the content, it may continue to be available on Dropbox's servers for a certain period of time.

25. In my training and experience, I have learned that Dropbox provides a "cloud" based storage service to the public. Given Dropbox's subscription practices, Dropbox's computers are likely to contain stored data (including photographs, videos, documents, applications, music, and other content) and information concerning subscribers and their use of Dropbox services, such as account access information, registration email account, and account application information. In my training and experience, such information may constitute evidence of a crime under investigation because the information can be used to identify the account user and images and videos contained within the account may contain child pornography.

26. In my training and experience, cloud storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.,* session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as IP addresses from which the account was accessed and/or registered), and other log files that reflect usage of the account. Because every device utilizes an IP address to connect to the internet, IP address information can help identify which computers or devices were used to access the Dropbox account.

27. Based on my training and experience, I also know the following:

a. People who have a history of and interest in sexual encounters with children will likely collect sexually explicit and suggestive material consisting of photographs, videos, and visual depictions of minors with whom they have had sexual contact and of other minors who stimulate their own sexual gratification, and they are likely to have these materials in their possession and/or stored in their email or online accounts.

b. People who have a history of and interest in sexual encounters with children will likely have records detailing communications with minors and other correspondence (with minors or adults) or records discussing sexual activity

involving minors. Bienvenue in this case admitted to having sexually explicit conversations with minor children over Snapchat, and there is evidence that he saved at least some of the material he collected over Snapchat to Dropbox.

c. People who collect child pornography almost always store these images on computers and other computer equipment, including web-based storage, and storage media capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and backing up electronic data. Such persons rarely, if ever, dispose of their sexually explicit materials, especially when they themselves have taken the photographs or made the videos, as these materials are considered prized possessions.

LEGAL AUTHORITY

28. The government may obtain both electronic communications and subscriber information from a provider of electronic communication services and remote computing services by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

29. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18, United States Code, Sections 2711, 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A). Specifically, the Court is "a district court of the United States…that – has jurisdiction over the offense being investigated," Title 18, United States Code, Section 2711(3)(A)(i). Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

30. If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

31. Because the warrants will be served on Dropbox who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

32. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Section 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment B, Sections I and II. Upon receipt of that information, government-authorized persons will review that information to locate the items described in Attachment B, Section III.

33. Because voluminous amounts of information can be stored in a cloud storage account, and because it might be stored in a deceptive order or with deceptive file names to conceal criminal activity, the searching authorities must examine all the stored data to determine which files constitute evidence, fruits, or instrumentalities of the crime. This sorting process can be very time-consuming and would be impractical to do at Dropbox's offices. Moreover, the sorting process should be done in a controlled environment because of the vast array of computer hardware and software that might be necessary even for computer experts to analyze the data, in order to ensure the integrity of the data recovered. Therefore, I request authority to seize all content and other records as more fully set forth in Attachment B, including any attached files, and other communications stored in this account, to be searched off site.

34. This application seeks warrants to search all responsive records and information under the control of Dropbox, a provider subject to the jurisdiction of this court, regardless of where Dropbox has chosen to store such information. Pursuant to Title 18, United States Code, Section 2713, the government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is

within Dropbox's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside of the United States.

REQUEST TO SEAL AND PRECLUDE NOTICE TO THE SUBSCRIBER(S)

35. I request that these applications, the warrants, the orders, and any related papers be sealed by the Court until such time as the Court pursuant to Local Rule 7.2 directs otherwise.

36. I further request that, pursuant to 18 U.S.C. §§ 2705(b) and 2703(b)(1)(A), the Court order Dropbox not to notify any person (including the subscribers or customers to which the materials relate) of the existence of this application, the warrant, the Order, or the execution of the warrant for the earlier of one year from the date of the court's order or upon notice by the government within 30 days of the conclusion of its investigation, unless the court extends such period under Title 18, United States Code, Section 2705(b). Although Bienvenue is aware of this investigation, non-disclosure is nevertheless appropriate in this case because the court's order relates to a still-ongoing criminal investigation that could identify other potential targets of the investigation, and its disclosure may alert these targets to the existence of the investigation. Moreover, some of the evidence in this investigation is stored electronically. If alerted to the existence of the order, the targets, including Bienvenue through a third party, could destroy that evidence, including information saved to their personal computing devices, on other electronic media, or in social media accounts. Accordingly, there is reason to believe that notification of the existence of the order could jeopardize the investigation, including by giving additional targets an opportunity to flee prosecution, destroy or tamper with evidence, change patterns of behavior, or intimidate potential witnesses. *See* 18 U.S.C. § 2705(b).

FOURTEEN-DAY RULE FOR EXECUTION OF WARRANT

37. Federal Rules of Criminal Procedure 41(e)(2)(A) and (B) direct the United States to execute a search warrant for electronic evidence within fourteen (14) days of the warrant's issuance. If the Court issues this warrant, the United States will execute it not by entering the premises of Dropbox, as with a conventional warrant, but rather by serving a copy of the warrant on the respective companies and awaiting their production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto internet companies' physical premises and the resulting disruption of their business practices.

38. Based on the training and experience of myself and other law enforcement agents, I understand that electronic account providers sometimes produce data in response to a search warrant outside the 14-day period set forth in Rule 41 for execution of a warrant. I also understand that electronic account providers sometimes produce data that was created or received after this 14-day deadline ("late-created data").

39. The United States does not ask for this extra data or participate in its production.

40. Should Dropbox produce late-created data in response to this warrant, I request permission to view all late-created data that was created by Dropbox, including subscriber, IP address, log records, and other transactional data, without a further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as messages, absent a follow-up warrant.

41. For these reasons, I request that the Court approve the procedures in Attachment B associated with the SUBJECT DROPBOX ACCOUNT which set forth these limitations.

CONCLUSION

42. Based on all of the foregoing, I submit that there is probable cause to believe that records and data from the SUBJECT DROPBOX ACCOUNT, as described in Attachment A, contain evidence of the commission of the SUBJECT OFFENSES, contraband, fruits of crimes, and things otherwise criminally possessed, and property designed and intended for use, and that has been used, as a means of committing the SUBJECT OFFENSES, as described in Attachment B, and request that the Court issue the requested search warrant.

Sworn to under the pains and penalties of perjury,

Jason J. DeFreitas

Special Agent Jason J. DeFreitas
Homeland Security Investigations

Subscribed and sworn to via telephone in accordance with Federal Rule of Criminal Procedure 4.1 on March 25, 2020.

HONORABLE JENNIFER C. BOAL
UNITED STATES MAGISTRATE JUDGE